



DVOMESTNA OPERACIJA

Dvomestna operacija na $S^{\text{množici}}$ je preslikava $S \times S \rightarrow S$.

Zunanja binarna operacija je preslikava $K \times S \rightarrow S$, npr.

množenje vektorja s skalarem $(\lambda, \vec{x}) \mapsto \lambda \vec{x}$ in $\mathbb{R} \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$.

Primeri dvomestne operacije: sčevanje na \mathbb{Z} , množenje na \mathbb{Z} , kompositum na $\mathcal{F}(X) = \{f: X \rightarrow X\}$.

Neutralni element e : $e * x = x * e = x$ za vsak $x \in S$.

(Indi levi in desni neutralni elementi. Če obstajata levi in desni neutralni elementi, sta enaka in $e_l = e_d = e$.)

Asociativnost: $x * (y * z) = (x * y) * z$.

Komutativnost: vsaka elementa $x, y \in S$ komutira: $x * y = y * x$.

POLGRUPE

Polgrupa je množica S skupaj z asociativno binarno operacijo $*$: $(S, *)$. Polgrupa z neutralnim elementom je monoid. $(\mathbb{N} \cup \{0\}, +)$ je monoid, $(\mathbb{N}, +)$ je polgrupa.

V monoidu majajo elementi lahko desne ali leve inverse:

$l^{-1} * x = e$, $x * r^{-1} = e$. Če ima x levi in desni inverse, je enake in en sam, tedaj je x obrnjen in $x * x^{-1} = x^{-1} * x = e$.

• X končna množica: $f: X \rightarrow X$ je injektivna \Leftrightarrow surjektivna \Leftrightarrow bijektivna.

• $T: X \times Y$ obrnjeva $\Rightarrow x * y$ je obrnjevo $(x * y)^{-1} = y^{-1} * x^{-1}$

• Pravilo krajevanja: če y obrnjevo, ie $x * y = x * z$ sledi $y = z$. (Indi je $y * x = z * x$)

GRUPE: OSNOVNE LASTNOSTI IN PRIMERI



Množica G skupaj z binarno operacijo $(x,y) \rightarrow xy$ je grupa, če je operacija asociativna, obstaja neutralni element (enota) in je vsak element obrniljiv.

Če je operacija v grupi komutativna, jo označujemo s $+$ in pravimo da je grupa Abelova.

Množica vseh obrniljivih elementov monoida (prologrpe z enoto) je grupa, tj. $S^* = \{x \in S \mid x \text{ je obrniljiv}\}$ je grupa. ($\mathbb{Z}^* = \{-1, 1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $(R^* = R \setminus \{0\}, \cdot)$, $(C^* = C \setminus \{0\}, \cdot)$).

$\mathcal{F}(X)$ je množica funkcij $f: X \rightarrow X$, $\mathcal{F}(X)^* = \{\text{bijektivne funkcije } X \rightarrow X\}$, kar označimo $\text{Sym}(X)$. $S_m = \text{Sym}(\{1, 2, \dots, m\})$ je grupa permutacij (končne množice).

Diederolska grupa: n -kotnik, $n \geq 3$, množica vseh simetrij je $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, z, rz, \dots, r^{n-1}z\}$, $r^n = 1$, $z^2 = 1$, $(rz)^2 = 1$.

Posledice Lagrangevega izreka: red vsakega elementa deli red grupe, $a^{161} = 1$. Mali Fermatov izrek: $a^p \equiv a \pmod p$ za vsa $a \in \mathbb{Z}/p\mathbb{Z}$ in $a \neq 0$.

$\mathbb{Z}/p\mathbb{Z}$ so cikличne (p prostovrstne) in matematične od končnih grup nisojo pravih metriskevih podgrup. ENOSTAVNA GRUPA - nima pravih metriskevih edinstv. \rightarrow npr. od abelovih le $\mathbb{Z}/p\mathbb{Z}$, A_n za $n \geq 5, \dots$ \rightarrow počasi Takih je 18 neshomogenevih dometov in 26 sporadičnih grup.

Concluzija izrek: G končna grupa, $p \mid |G| \Rightarrow G$ vsebuje element reda p .

p -grupa je grupa, v kateri je red vsakega elementa potenca prostovrstila p .

1: Vsaka končna Abelova grupa je direktna mesta cikличnih podgrup. Te podgrupe lahko imenujemo tako, da so njihovi redi potence prostovrstil.



KOLOBARJI: OSNOVNE LASTNOSTI IN PRIMERI

Holobar je množica $(K, +, \cdot)$, bei je za sestevanje Abelova gruba, množenje je asociativno (naši definicije oblikujejo tudi, da vsebuje enoto 1 za množenje), in veljata distributivnostna zakona $x(y+z) = xy+xz$ in $(y+z)x = yx+zx$.

Lastnosti: $0_x = x0 = 0$, $(-x)y = x(-y) = -xy$, $(x-y)z = xz-yz$, $z(x-y) = zx-zy$, $(-x)(-y) = xy$, $(-1)x = x(-1) = -x$

Če je množenje komutativno, rečemo, da je holobar komutativen.

Ničelni (trivialni) holobar: $\{0\}$. $K=\{0\} \Leftrightarrow 0=1$

$M_n(\mathbb{R}) = \mathbb{R}^{n \times n}$ je množica realnih matrik velikosti $n \times n$ in je holobar za običajno matično sestevanje in množenje. Množenje ni komutativno. Obstaja pa delitelji niča: $AB=0$ in $A \neq 0, B \neq 0$.

Element $x \neq 0$ je delitelj niča, če obstaja $y \neq 0$, da je $xy=0$ ali $yx=0$. Če holobar je komutativen holobar brez deliteljev niča. Obsteg je neničelni holobar, v katerem je vsak od 0 različen element obrnljiv.

Pošte je komutativen obseg. Kpr. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p, GF(4), GF(2)$

T: Obrnljiv element ni delitelj niča. Zato obseg ne vsebujejo deliteljev niča. D: $xy=0 \rightarrow x^{-1}xy=0 \rightarrow y=0$

Primer: \mathbb{Z} je holobar, ni obseg, nima deliteljev niča.

Algebra je holobar in vektorski prostor. $+$, \cdot , množenje s skalarjem. "Algebra je malo boljši holobar."

CIKLICKE GRUPE



Ciklicka grupa je grupa, ki je generirana s enim samim elementom.

$$G = \langle a \rangle = \{a^n; n \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, a^3, \dots\}$$

Npr. $(\mathbb{Z}, +)$, $(\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}, +)$, množini enot v \mathbb{C}

T: Vraka ciklicka grupa je izomorfna bodisi $(\mathbb{Z}, +)$ bodisi $(\mathbb{Z}_n, +)$ za neki $n \in \mathbb{N}$.

D: Če mi niholi $a^k = a^l$, je $\varphi: \mathbb{Z} \rightarrow \langle a \rangle$, $\varphi(n) = a^n$ inj. in surj, torej izomorfizem gru. Če pa obstaja $a^k = a^l$, poiščemo min $k-l > 0$, torej $a^{k-l} = 1$ in $\varphi(n) = a^m$, $\varphi: \mathbb{Z}_n \rightarrow \langle a \rangle$.

Element $a \in G$ ima končen red, če je $a^n = 1$ za neki $n \in \mathbb{N}$.
čajmanjšemu takemu s pravimo red elementa. Če
 $a^n \neq 1$ za vsek $n \in \mathbb{N}$, ima a neskončen red. Če je
grupa končna, tj. $|G| < \infty$, ima vsak element končen red.

Primer: v \mathbb{Z}_4 imata 1 in 3 red 4, 2 imas red 2, 0 imas red 1.

V \mathbb{Z} imajo vse elementi razen 0 neskončen red. V $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

ima $(0,0)$ red 1, $(0,1), (1,0)$ in $(1,1)$ pa red 2. Ester \mathbb{Z}_4 in

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ niso izomorfnii gruji. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ ni ciklicka grupa.

Če imas a red n, je $\langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$ in
red a = red $\langle a \rangle$.



POLJE (OBSEG) ULOMKOV

Vrah cel broobar (komutativen brez deliteljev nica)
lahko vložimo v polje.

Vpeljemo relacijo na $K \times K \setminus \{0\}$: $(a, b) \sim (c, d) \Leftrightarrow ad = bc$.
 \sim je ekvivalenčna relacija (refl., sim., trans.) in vpeljemo
ekvivalenčne množice $\frac{a}{b} = [(a, b)]$.

1: Naj bo K cel broobar. V množico vseh ekvivalenčnih
množic množic $F_K := \left\{ \frac{a}{b} ; a, b \in K, b \neq 0 \right\}$ vpeljemo + in
· predpisom $\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$ in $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Potem
je F_K polje, preslikava $a \mapsto \frac{a}{1}$ pa vložimo K v F_K .

D: Preverimo dobro definiranost + in ·, zg. iz $\frac{a}{b} = \frac{a'}{b'}$ in $\frac{c}{d} = \frac{c'}{d'}$ sledi
 $\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$ in $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. Preveriti bi morali še avocija + in ·,

distributivnost. $1 = \frac{1}{1}$, $0 = \frac{0}{1}$, $-\frac{a}{b} = \frac{-a}{b}$, $(\frac{a}{b})^{-1} = \frac{b}{a}$, če $a \neq 0$

$\varphi: K \rightarrow F_K$, $\varphi(a) = \frac{a}{1}$, $\varphi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$.

Polje F_K imenujemo polje ulomkov holobarja K .

Primeri: 1) $K = \mathbb{Z} \Rightarrow F_K = \mathbb{Q}$. 2) Če je K že polje, je $F_K = K$ in

$a = \frac{a}{1}$. 3) Polinomi $F[X]$ nad poljem F . Holobar $K = F[X]$ je cel.

$F(X)$ je polje racionalnih funkcij $\frac{f(x)}{g(x)}$, $g(x) \neq 0$.

4) $K = \mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \rightsquigarrow F_K = \mathbb{Q}(i) = \{p+qi \mid p, q \in \mathbb{Q}\}$

KARAKTERISTIKA



Karakteristika holobarja je najmanjše naravno število n z lastnostjo $n \cdot 1 = 0$. $1, 2 \cdot 1 = 1+1, 3 \cdot 1 = 1+1+1, \dots$

v neholobrih holobarjih pridemo do $n \cdot 1 = 1+1+\dots+1 = 0$.

Če takega n ni, rečemo, da ima holobar karakteristiko 0. $\mathbb{Z}, \mathbb{Q}, \mathbb{R} \dots$ imajo karakteristiko 0.

\mathbb{Z}_n ima karakteristiko n , pa tudi $\mathbb{Z}_n[x], M_n(\mathbb{Z}_n)$,

$\mathbb{Z}_n \times \mathbb{Z}_m$ imajo karakteristiko n . $\mathbb{Z}_p(X)$ je polje racionalnih funkcij s koeficienti iz \mathbb{Z}_p in je primer meskovičnega polja s karakteristiko p . Karakteristika holobarja $\mathbb{Z}_m \times \mathbb{Z}_n$ je $\text{v}(m, n)$.

Če ima K karakteristiko $n > 0$, je $n \cdot x = 0$ za vsa $x \in K$.

Karakteristika holobarja brez določiljev nica je 0 ali paštevko.

I: Če ima polje F karakteristiko 0, obstaja vločitev $\mathbb{Q} \rightarrow F$. Če ima polje F karakteristiko p (paštevilo), obstaja vločitev $\mathbb{Z}_p \rightarrow F$.

D: V prem primerni $\Psi: \mathbb{Q} \rightarrow F$, $\Psi\left(\frac{m}{n}\right) = (m \cdot 1) \cdot (n \cdot 1)^{-1}$, v drugem $\Psi: \mathbb{Z}_p \rightarrow F$, $p \cdot 1 = 0$, $\Psi([k]) = k \cdot 1$. Preverimo dobro definiranost, da je homomorfizem holobarjov in da je Ψ injektivna. $\rightarrow \ker \Psi = [0]$

Pravpolje polja F je podpolje polja F , generirano z 1.

To je najmanjše podpolje polja F . Če ima F karakteristiko 0, je njeno pravpolje izomorfno \mathbb{Q} , če ima karakteristiko p , je njeno pravpolje izomorfno \mathbb{Z}_p .



PODGRUPE, ODSEKI, LAGRANGEV IZREK

Napravna podmnožica H grupe G je podgrupa, če je za vse $x, y \in H$ tudi $xy^{-1} \in H$ oz. če $x, y \in H$ je xy in $x^{-1} \in H$.

$\{h \in G \mid ah = ha \}$ je prava podgrupa.

Za vsak $a \in G$ je $aH = \{ah \mid h \in H\}$ ODSEK grupe G po podgrupi H . Aditivni primer: $a + H = \{a + h \mid h \in H\}$. $a \in H \Leftrightarrow aH = H$, nato pa je aH ni podgrupa. Če sledimo le leve odselje (denki bi bili Ha).

Primer: 1) $G = \mathbb{Z}$, $H = m\mathbb{Z}$. Odseli: $n\mathbb{Z}, 1+m\mathbb{Z}, 2+m\mathbb{Z}, \dots, n-1+m\mathbb{Z}$, kar so ravno $[0], [1], \dots, [n-1]$ oz. elementi \mathbb{Z}_n .

2) $G = \mathbb{R}^2$, $H = \text{osx}$, odseli so vodoravne premice. 3) $G = \mathbb{C}$, $H = \mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$, odseli so krožnice srediscem v 0 ta ni podgrupa

4) $G = S_n$, $H = A_n$, odsela sta podle permutacij A_n in like permutacije.

T: $aH = bH \Leftrightarrow b^{-1}a \in H$. Aditivno: $a+H = b+H \Leftrightarrow a-b \in H$

T: Odsela aH in bH sta enaka ali disjunktna. Torej imamo particijo G na disjunktne odselje.

Indeks podgrupe H je število vseh odselkov aH , označa $[G : H]$. Primer $[\mathbb{Z} : m\mathbb{Z}] = m$.

Lagrangev izrek: Če $H \leq G$ je $|G| = [G : H] \cdot |H|$. Torej število elementov podgrupe deli število elementov grupe.

D: $h \mapsto ah$ je bijekcija, tako da nini odseli moči $|H|$.



EDINICE, KVOCIENTNA GRUPA IN

HOMOMORFIZMI GRUP

Podgrupa N grupe G je edinica, če za vse $a \in G$ in $n \in N$ velja $ana^{-1} \in N$. Vralka $N \trianglelefteq G$. Ekvivalentno $aNa^{-1} \subseteq N$, $aN \cap Na = N$, $aNa^{-1} = N$.

Primer: v Abelovi grupi je vsaka podgrupa tudi edinica, matrice $\det=1$ v grupi obrnljivih matrice (SL_n v GL_n), sede permutacij v grupi vseh permutacij (A_n v S_n).

Naj bo $N \trianglelefteq G$. Potem je množica vseh odsekov, $G/N = \{aN \mid a \in G\}$, grupa za operacijo $aN \cdot bN = (ab)N$.

Predstavitev $\pi: G \rightarrow G/N$, $\pi(a) = aN$, je epimorfizem in $\ker \pi = N$. D: Dobro def. množenja, avoc., enota $1N=N$, inverz $(aN)^{-1} = a^{-1}N$, nuj. G/N je kvocientna grupa, π je kanonični epimorfizem.

T: $N \trianglelefteq G$ je podgrupa edinica $\Leftrightarrow N = \ker \psi$ za neki homomorfizem $\psi: G \rightarrow G'$.

Proizvod grup $H, K \trianglelefteq G$ je $HK = \{hk \mid h \in H, k \in K\}$, v splošnem ni podgrupa.

T: $\forall H, K \trianglelefteq G$ m $HK = KH \Rightarrow HK \trianglelefteq G$. $\forall H \trianglelefteq G$ in $N \trianglelefteq G \Rightarrow HN = NH \trianglelefteq G$.

c) $M, N \trianglelefteq G \Rightarrow MN \trianglelefteq G$. d) $M, N \trianglelefteq G$ in $M \cap N = \{1\} \Rightarrow mn = nm \quad \forall m \in M \quad \forall n \in N$.

Eje $H \trianglelefteq G$ in $N \trianglelefteq H$, je $N \trianglelefteq G$ in $H/N \leq G/N$.

T: Naj bo $\psi: G \rightarrow G'$ homomorfizem grupe. a) Brasilita podgrupe je podgrupa, $H' \trianglelefteq G' \Rightarrow \psi^{-1}(H') \trianglelefteq G$. b) $N' \trianglelefteq G' \Rightarrow \psi^{-1}(N') \trianglelefteq G$. c) $H \trianglelefteq G \Rightarrow \psi(H) \trianglelefteq G'$.

d) $N \trianglelefteq G$ in ψ epimorfizem $\Rightarrow \psi(N) \trianglelefteq G'$.

T: Naj bo $N \trianglelefteq G$. Vralka podgrupa G/N je oblike H/N , kjer $H \trianglelefteq G$ in $N \trianglelefteq H$. Vralka podgrupa edinica G/N je oblike M/N , kjer $N \trianglelefteq G$ in $M \subseteq N$.



PODKOLOBARJI IN IDEALI

Podmnožica L holobarja K je podholobar, če vsebuje enoto 1 holobarja K in je za vsi operaciji sama holobar.

$\{[x \ 0] | x \in \mathbb{R}\}$ je holobar za množični operaciji, a ni podholobar 2×2 realnih matrik $M_2(\mathbb{R})$, ker je enota $[0 \ 0]$ različna od $[0 \ 1] \in M_2(\mathbb{R})$.

$T: L$ podholobar $\Leftrightarrow 1 \in L$, $xy \in L$ in $x-y \in L$ za $x, y \in L$.

Najmanjši holobar, ki vsebuje 1, je \mathbb{Z} . $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Center holobarja $Z(K) = \{c \in K \mid cx = xc \text{ za } \forall x \in K\}$ vse elementi, ki so vsebuju homotrop.

Podmnožica I holobarja K je ideal, oznaka $I \triangleleft K$, če velja: I je podgrupa za sestevanje ($x-y \in I$ za $x, y \in I$) in $xu \in I$ ter $ux \in I$ za $\forall x \in K$ in $\forall u \in I$, torej $IK \subseteq I$ in $KI \subseteq I$.

Primer: $\{0\} \triangleleft K$, $K \triangleleft K$. $K = \mathbb{Z}$, $I = m\mathbb{Z}$ je grupa za $+$: $(a+I) + (b+I) = (a+b)+I$:
 $(a+m\mathbb{Z}) + (b+m\mathbb{Z}) = ab + m\mathbb{Z}$

$$[a] + [b] = [a+b] \text{ in } (a+I)(b+I) = ab + I; [a] \cdot [b] = [ab]$$

Naj bo K komutativen (množenje je komutativno). Za vsak $a \in K$ je $(a) = aK = \{ax \mid x \in K\}$ ideal holobarja K , imenovan glavni ideal.

Ideali v splošnem niso holobarji, ker ne vsebujejo enote (za množenje).

T : Če sta $I, J \triangleleft K$, so ideali tudi $I \cap J$, $I+J = \{u+v \mid u \in I, v \in J\}$, $IJ = \{u_1v_1 + \dots + u_nv_n \mid u_i \in I, v_j \in J, n \in \mathbb{N}\}$. $IJ \subseteq I \cap J \subseteq I \subseteq I+J$.

$$I = 4\mathbb{Z}, J = 6\mathbb{Z}: I \cap J = 12\mathbb{Z}, I+J = 2\mathbb{Z}, IJ = 24\mathbb{Z}$$

KVOCIENTNI KOLOBAR IN HOMOMORFIZMI

KOLOBARJEV



Naj bo $I \triangleleft K$. Množica vseh odsekov, $K/I = \{a+I, a \in K\}$, je kolobar s operacijama $(a+I) + (b+I) = (a+b)+I$ in $(a+I)(b+I) = ab+I$. Preslikava $\pi: K \rightarrow K/I$, $\pi(a) = a+I$, je kanonični epimorfizem kolobarjev, ker $\pi = I$ in K/I je kvocientni kolobar. D: Vemo, da je K/I grupa za +, preverimo dobro def. množ., avoc. mn., distr., $O_{K/I} = I$, $1_{K/I} = 1_K + I$, $\pi(ab) = \pi(a)\pi(b)$. \Rightarrow ideal je lev in desni ideal librat.

"Obstajajo enostranski" (levi oz. desni) ideali: L podgrupa za restovanje in velja $KL \subseteq L$ (ne pa $LK \subseteq L$). Če je $x \in L$ levični obratljiv element, je $L = K$ (naj takrat $l \cdot l^{-1} = 1 \in L$ in $ex \in K \Rightarrow x \cdot 1 \in L$).

Kolobar $\stackrel{K \neq \{0\}}{\text{je obseg} \Leftrightarrow \{0\}}$ in K sta njegova edina leva idealna, $\stackrel{\text{oz. desna}}{\text{Kolobar je enostaven, če } K \neq \{0\}}$ in sta $\{0\}$ in K njegova edina idealna. Vsi obsegi so enostavni. Matice $M_n(F)$

Komutativen kolobar $K \neq \{0\}$ je polje $\Leftrightarrow K$ je enostaven.

T: $\psi: K \rightarrow K'$ homomorfizem kolobarjev. a) $I' \triangleleft K' \Rightarrow \psi^{-1}(I') \triangleleft K$. b) $I \triangleleft K$ in ψ epimorfizem ($\stackrel{\text{tanj}}{\text{surjektiv}} \Rightarrow \psi(I) \triangleleft K'$)

I: Če je $I \triangleleft K$, je vsak ideal kvocientnega kolobara K/I oblike J/I , kjer je J ideal kolobara K, ki vsebuje I (tj. $I \subseteq J \triangleleft K$).

I $\triangleleft K$ je maksimalen ideal, če $I \neq K$ in če ne obstaja tak J $\triangleleft K$, da bi nelpo I $\subsetneq J \triangleleft K$.

I $\triangleleft K$ je maksimalen $\Leftrightarrow K/I$ je enostaven.

K komutativen: $I \triangleleft K$ maksimalen $\Leftrightarrow K/I$ je polje.



IZREK O IZOMORFIZMU

Naj bo $\varphi: A \rightarrow A'$ homomorfizem (česarhol).

Ton je $A/\ker\varphi \cong \text{Im } \varphi$.

D: $\ker\varphi$ je edinica, ideal, rektorski podprostor... cato na definicija splet s njej. Dolazak sa A u A' grupi.

$a\ker\varphi = a'\ker\varphi \Leftrightarrow \dots \Leftrightarrow \varphi(a) = \varphi(a')$ in definiramo

$\bar{\varphi}: A/\ker\varphi \rightarrow \text{Im } \varphi$, $\bar{\varphi}(a\ker\varphi) = \varphi(a)$ dobra def. in inj.,
sug. očitno, $\bar{\varphi}(a\ker\varphi \cdot b\ker\varphi) = \bar{\varphi}((ab)\ker\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(a\ker\varphi) \cdot \bar{\varphi}(b\ker\varphi)$.

Za holobar bi bilo $\bar{\varphi}(a + \ker\varphi) = \varphi(a)$.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \\ \pi \downarrow & \nearrow \bar{\varphi} & \\ A/\ker\varphi & \xrightarrow{\bar{\varphi}} & \text{Im } \varphi = \varphi \circ \pi \end{array}$$

Primeri: $G/G \cong \{1\}$; $G/\{1\} \cong G$; $G = \mathbb{R}^2$, $H = x, 03$, $G/H \cong \mathbb{R}$;

$G = \mathbb{C}^*$, $H = \mathbb{T} = \{z \in \mathbb{C}; |z|=1\}$, $G/H = \mathbb{R}^+$, $\varphi(z) = |z|$;

$G = GL_n(\mathbb{R})$, $H = SL_n(\mathbb{R})$, $\varphi(A) = \det A$, $G/H = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$;

$G = S_m$, $H = A_m$, $G/H = \mathbb{Z}_2 = \{-1, 1\}$.

Kolobarji: $\mathbb{K}/(03) \cong \mathbb{K}$; $\mathbb{K}/\mathbb{K} \cong \{03\}$; $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$

Ekvivalentno je: p je prostervis, \mathbb{Z}_p je polje, $p\mathbb{Z}$ je maksimalni ideal.

• \mathbb{K} kolobar $\Rightarrow \mathbb{K}[x]$ kolobar polinomov, $I = X \mathbb{K}[x]$ je polinomi s konstantnim členom 0, $\varphi(a_0 + a_1x + \dots + a_nx^n) = a_0$, $\mathbb{K}[x]/I \cong \mathbb{K}$.

\mathbb{K} je \mathbb{K} komutativen, lahko evaluiramo $\varphi(f(x)) = f(0)$.

• $C[a,b]$, $c \in [a,b]$ $\varphi: C[a,b] \rightarrow \mathbb{R}$, $\varphi(f) = f(c)$ je homomorfizem

slagber, $I = \ker\varphi = \{f \mid f(c)=0\} \triangleleft C[a,b]$, $C[a,b]/I \cong \mathbb{R}$, I maksimaln, ker je \mathbb{R} polj.

p prvelement $p \neq 0$, ni obrnjev, p lab \Rightarrow pla ali plb. Glavni kolobar je nevarcep $\Leftrightarrow p$ prvelement.
Vsak glavni kolobar je **kolobar z enolično faktorizacijo**. - za \mathbb{Z} je to osnovni
vrstni aritmetični. Enoličen produkt nevarcenih elementov.



KOLOBARJI POLINOMOV

Dolamo teorijo komutativnih kolobarjev. Uvodna razbera sta \mathbb{Z} in $F[x]$,
da komutativa, brez deliteljev niso, niso polji, v \mathbb{Z} obstajajo b^{-1} in 1 , v $F[x]$ pa niso.

Uvodni izrek o deljenju polinomov: $f(x), g(x) \in F[x], g(x) \neq 0$. Obstaja polje
takša $q(x)$ in $r(x)$, da je $f(x) = g(x) \cdot q(x) + r(x)$, $st(r(x)) < st(g(x))$ ali $r(x) = 0$.

P: $a \in F$ je **ničla** polinoma $f(x) \Leftrightarrow (x-a)$ deli $f(x)$. **Nerazcepni polinom:**
nekonstantni in ga ne moremo zapisati kot produkt dveh nekonstantnih polinomov.

x^2+1 nerazcepni nad \mathbb{R} , varcepni nad \mathbb{C} . Uvodni vrstni algoritri \Rightarrow nad \mathbb{Q}
so varcepni le linearni polinomi, nad \mathbb{R} linearni in kvadratni $\Rightarrow b^2 - 4ac < 0$.

Elmenti polinomov nad \mathbb{Q} lahko podamo b nad \mathbb{Z} (množimo s ustreznim celim številom).

$p(x) \in \mathbb{Z}[x]$ je **primitiven**, če je največji stopnji delitev njenih koeficientov enak 1.

Prodot dveh primitivnih polinomov je primitiven. Če $f(x) \in \mathbb{Z}[x]$ ne moremo
razcepiti na produkt v $\mathbb{Z}[x]$, je nerazcepni nad \mathbb{Q} . **Eisensteinijev kriterij:**

Naj bo $f(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$. Če obstaja pravštevilo p , ki deli a_0, a_1, \dots, a_{n-1} , ne
pa a_n in p^2 ne deli a_0 , je $f(x)$ nerazcepni nad \mathbb{Q} . Npr. $f(x) = x^3 - p$ je nerazcepni
nad \mathbb{Q} .

DELJIVOST V KOMUTATIVNIH KOLOBARJIH $bla \Leftrightarrow a = b \cdot q, q \in \mathbb{Z}$. $a, b \in \mathbb{Z}, b \neq 0$

a in b sta si **asociirana** $\Leftrightarrow a b \in bla$. p **nerazcepni element**: $p \neq 0$, pri obnifik
in je $p = a \cdot b$ sledi $a \mid b$ je obnifik. d n.z.d. od $a \mid b$: $d \mid a, d \mid b$, če $d \mid a \mid b \Rightarrow d \mid b$.

$D(a, b) = 1 \Rightarrow a, b$ sta si **tuja**. Polje: vsaka nonična elementa sta si asociirana. **Glavni ideal**: generiran je enim razum elementom; $(a) = \{ax \mid x \in \mathbb{Z}\}$. $(a) = (b) \Leftrightarrow a, b$ asociirana.

Polinomi več spremenljivk: $X, Y \in F[X, Y] \rightarrow (X, Y)$ ni glavni ideal, X, Y sta si tuja.

Glavni kolobar - vsak njegov ideal je glavni, npr. \mathbb{Z} in $F[x]$. **Euclidski kolobar** - v njen je
mleči verziji vsaka o deljenju, $\delta(r) \subset \delta(b)$. Euclidski a. je glavni, npr. $\mathbb{Z}, F[x], \mathbb{Z}[x]$ Gaussova rešitev,
 $F[[x]]$ formalne potencije vstv. T: \forall glavni kolobar. Potem p nerazcepni $\Leftrightarrow (p)$ mleč. ideal $\Leftrightarrow k/(p)$ je polje.



OBSEGI, POLJA: OSNOVNE LASTNOSTI IN PRIMERI

Obseg je neničeliščni kolobar, v katerem je vsak od 0 različen element obrniljiv. Polje je komutativen obseg.

Glavni primeri: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Med \mathbb{Q} in \mathbb{R} je še veliko drugih polj, npr. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Obsegi nimajo deliteljev ničila.

Končna polja: \mathbb{Z}_p , p praštevilo. ($\in \text{GF}(p^n)$)

Pole ułomkov $\leadsto \mathbb{Q}$.

Racionalne funkcije $\rightarrow F(x)$. $\mathbb{Q}(x) = \{p + qx \mid p, q \in \mathbb{Q}\}$

Ta je druga filozofija, običajno ne iščemo podpolj, ampak razširitev polj.

Polje je kolobar, zato ima karakteristiko. Če ima karakteristiko 0, varj lahko vločimo \mathbb{Q} . Če ima karakteristiko p , varj lahko vločimo \mathbb{Z}_p .

RAZŠIRITVE (NADALJEVANJE)

1. Če so $a_1, a_2, \dots, a_n \in E$ algebraični nad F , je $F(a_1, \dots, a_n) = F[a_1, \dots, a_n]$

končna razširitev F

Primer: $\mathbb{Q}(\sqrt{2}) = \{a_0 + a_1\sqrt{2} \mid a_i \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2 \mid a_i \in \mathbb{Q}\}$,

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} \mid a_i \in \mathbb{Q}\}$, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

• Razširitev $F \Rightarrow$ množica vseh elementov $x \in E$, ki so algebraični nad F , je podpolje E . \rightarrow npr. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

tereko primitivnemu elementu: Vsaka končna razširitev polja s karakteristiko 0 je enostavno



KONČNE, ALGEBRAIČNE IN TRANSCENDENTNE RAZŠIRITVE

Naj bo a element razširitve E polja F . Če obstaja neničleni polinom $f(x) \in F[x]$, da je a ničla tega polinoma ($f(a)=0$), je a algebraičen nad F . Če pa je a transcendent.

Minimalni polinom za $a \in E$: $p(a)=0$, vodilni koef. je 1, ki med vseh takih ima najmanjšo stopnjo.

↪ je "moničen"

$$\text{je } f(a)=0,$$

$\cdot p(x)$ moničen, a algebraični element: $p(x)$ minimalen $\Leftrightarrow p(x)$ neverjeten $\Leftrightarrow p(x)$ deli $f(x)$

$\cdot a$ je algebraičen stopnje n : njegov minimalni polinom je stopnje n .

Primer: vsak $a \in F$ je algebraičen stopnje 1; $F=\mathbb{R}$, $E=\mathbb{C}$, $z \in \mathbb{C} \setminus \mathbb{R}$ je algebraičen stopnje 2;

F polji, $E=F(x)$, x je transcendent nad F , $F=\mathbb{Q}$, $\sqrt[n]{p}$ je algebraičen stopnje n .

π, e sta transcendentni števili, sa $\pi + e$ se niti ne ve, če je racionalno.

Razširitev lahko obravnavamo kot vektorski prostor nad F , $\forall x, z \in F, x \in E$.

Končna razširitev: E kot vektorski prostor nad F je končnorazširjen.

$\dim E = [E:F]$. T: $F \subseteq L \subseteq E$ končne razširitve $\Rightarrow [E:F] = [E:L] \cdot [L:F]$.

D: $\{a_1, \dots, a_m\}$ baza L nad F , $\{b_1, \dots, b_n\}$ baza E nad L , $\{a_i b_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ baza E nad F .

Razširitev E polja F je algebraična, če je vsak element iz E algebraičen nad F .

T: Vraka končna razširitev je algebraična. → Če pa je transcendentna.

D: $[E:F] = n$, tj. sa $a \in E$ obstaja polinom stopnje n , ki je na enak 0.

$\cdot F(a) = \{f(a) | f(x) \in F(x)\}$ je polje, generirano v F in a , $a \in E \Rightarrow F(a)$ podpolje E .

Polje E je enostavna razširitev polja F , če obstaja $a \in E$, da je $E = F(a)$. Potem

je a primitivni element razširitve E (ni enoličen).

I: Naj bo $a \in E$ algebraičen stopnje n . $F(a) = F[a] = \{x_0 + x_1 a + \dots + x_{n-1} a^{n-1} | x_i \in F\}$
in $[F(a):F] = n$.



RAZPADNO POLJE

Kratost nčle: $f(x) \in F[x]$, E razširovo. ki je kratost nčl. aice, če je $f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2} \dots (x-a_t)^{k_t}$ in $f_0(x) \in E$ nizn. nčl. Če je nekonstanten polinom $f(x) \in F[x]$ lahko zapisano kot produkt linearnih polinomov s koeficienti iz E , pravimo, da $f(x)$ razgradi v razširovi E polja F . Če ne razgradi v nobenem pravem podpolju polja E , je E razpadno-polje polinoma $f(x)$. Torej razpadno polje je najmanjša razširovka, ki vsebuje vse nčle polinoma $f(x)$.

I: Za vsak nekonstanten polinom $f(x) \in F[x]$ obstaja razpadno polje. Dokazali smo v bistvu ekvivalentno: F polip, $f(x) \in F[x]$ nekonstanten polinom. Potem obstaja razširovka E polja F , v kateri ima $f(x)$ nčlo.

D: Obstaja razcepjen $p(x)$, ki deli $f(x)$. Potem je $(p(x)) = I$ ideal in $E := F[x]/I$ polip. Vložimo $F \neq E$ je $\pi: x \mapsto x+I$. $X+I$ je nčla, saj je za polj. $g(x) = \sum_{i=0}^m g_i x^i$ $g(X+I) = \dots = g(x)+I$ in rato $f(X+I) = f(x)+I = I = 0+I$.

• Razpadno polje je odvisno od F . Za $f(x) = x^2 + 1$, je razpadno polje v primerih: $F = \mathbb{Q} \rightsquigarrow \mathbb{Q}(i) = \{g + ri | g, r \in \mathbb{Q}\}$, $F = \mathbb{R} \rightsquigarrow \mathbb{R}(i) = \mathbb{C}$, $F = \mathbb{C} \rightsquigarrow \mathbb{C}$, $F = \mathbb{Z}_2 \rightsquigarrow \mathbb{Z}_2$ (saj $x^2 + 1 = (x+1)^2$).

• Razpadno polje polinoma $f(x) \in F[x]$ je do izomorfizma enolično določeno. (Nekaj leva za to dokazati.)



ALGEBRAIČNO ZAPRTA POLJA,

OSNOVNI IZREK ALGEBRE

Vsek nekonstanten polinom s kompleksnimi koeficienti ima kompleksno ničlo.

Polje Z je algebraično zaprto, če ima vsek nekonstanten polinom $Z[x]$ vsaj eno ničlo v Z . Potem jih ima $\overset{v Z}{\exists}$ število, kot je stopnja tega polinoma, ve ničle in vodilni koef. so v Z : $f(x) = c(x-a_1) \cdots (x-a_n)$, $c, a_i \in Z$.

Primer: C .

E je L algebraična razširitev polja F , E pa alg. razš. polja L , in $x \in E$ algebraičen nad L , je x algebraičen tudi nad F .

P: Algebraična razširitev algebraične razšritve je algebraična.

Polje A je algebraično zaprtje polja F , če je algebraično zaprto in je algebraična razširitev polja F . C je alg. zaprtje za R , ne pa za Q , saj je razšritve iz Q v C transcendentne.

Naj bo Z algebraično zaprto polje in F njegovo podpolje.

Naj bo A množica vseh $z \in Z$, ki so algebraični nad F .

Potem je A algebraično zaprtje polja F .

Algebraično zaprtje polja Q je polje vseh algebraičnih števil. (Vse možne ničle polinomov s racionalnimi koeficienti.)

Za vsek polje F obstaja algebraično zaprtje in je do izomorfizma natomično določeno. (Nismo dokazali, sonoma...)

Vsnovega vrha algebe x ne da dokazati brez koncepta evnosti in analize.



KONČNA POLJA

\mathbb{Z}_p je polje za vrako prstevilo p . Če n ni prstevilo, \mathbb{Z}_n ni polje. Direktni produkt polj ni polje (vsi vsebuje delitelje nica). Končno polje ne more imeti karakteristike 0 , vsi točki vsebuje 0 , ki je neskončno. Zato ima vrako končno polje karakteristično p , p prstevilo, in vsebuje (izomorfno kopijo) \mathbb{Z}_p .

- E razsintez \mathbb{Z}_p ima karakteristiko p in mož $|E|=p^m$ eanchim.
 - Elementi so lin. komb. base $\{b_1, \dots, b_m\}$: $\alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_m b_m, \alpha_i \in \mathbb{Z}_p$. Imamo p^m različnih m-trov $(\alpha_1, \dots, \alpha_m)$. $[E : \mathbb{Z}_p] = m \Leftrightarrow |E| = p^m$.
 - $E \approx p^m$ elementi je napadno polje ca $f(x) = X^{p^m} - X$ nad \mathbb{Z}_p . Vsek element na red. grupe E^* , p^{m-1} , ip enak 1: $x^{p^{m-1}} = 1 \forall x \in E^*$, $x^{p^m} = x \forall x \in E$ (tudi za 0). Toto $f(x)$ napade v E in ne more razpasti v pravem podpolju E .
- Nad \mathbb{Z}_p veljajo brucove sanje $(x+y)^p = x^p + y^p$.

I: Za vrako prstevilo p in vrako naravno število m obstaja polje $GF(p^m)$ s p^m elementi. Vrako končno polje je izomorfno polju $GF(p^n)$ za neka $n \leq m$.

\oplus	\times	\oplus	\times
$\begin{array}{ c cccc }\hline 0 & 0 & 1 & a & 1+a \\ \hline 0 & 0 & 1 & a & 1+a \\ \hline 1 & 1 & 0 & 1+a & a \\ \hline a & a & 1+a & 0 & 1 \\ \hline 1+a & 1+a & a & 1 & 0 \\ \hline \end{array}$	$\begin{array}{ c ccccc }\hline 0 & 1 & a & 1+a & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & a & 1-a \\ \hline a & 0 & a & 1+a & 1 \\ \hline 1-a & 0 & 1+a & 1 & a \\ \hline \end{array}$		
$a^2 = 1+a$			

$$(1+a) \cdot a = a + 1+a = 1$$